## Remarks

The Office Action dated October 6, 2011, and made Final, and further in response to the Advisory Action dated December 13, 2011, have each been carefully reviewed and the foregoing Amendment and remarks have been made in consequence thereof.

Claims 1, 2, 6, 8, 10-15, 18-25, and 27-31 are now pending in this application. Claims 1, 2, 6, 8, 10-15, 18-25, and 27-31 stand rejected. Claims 3-5, 7, 9, 16, 17, and 26 have been canceled.

The rejection of Claims 1, 2, 6, 8, 10-15, 18-25, and 27-31 under 35 U.S.C. § 112, first paragraph is respectfully traversed. Applicants respectfully disagree with the assertion made on page 3 of the Action that there "is nothing in the specification to suggest that the data will simply not be deobfuscated when the configuration changes." Applicants respectfully submit that the originally-filed specification conveys to one having ordinary skill in the art that the Applicants possessed the claimed invention at the time the application was filed. More specifically, a person with ordinary skill in the art, taking the application as a whole, would have understood the specification to describe a method for transmitting data that is obfuscated to a subscriber.

The originally-filed application recites that a business entity may protect "proprietary data" using measures such as, but not limited to, "obfuscating the data before transmitting the data over a network" (*see* paragraph [0018]). The data may be "obfuscated at the data source" (*see* paragraph [0019]). A supervisory processor (304) is configured to execute software instructions based on a processor configuration (310), and may be coupled to a subscriber network segment (306) through a port (314) (*see* paragraph [0021]). Processor (304) "determines from configuration 310 whether to transmit the data to subscriber segment 306. Processor [304] may transmit the data to segment 306 by enabling port 314 to a transmit state . . . [and/or] deobfuscating the data at port 314 if the data is obfuscated" (*see* paragraph [0023]). The Office Action recites, on page 3, that it "is clear from this citation that the port through which the data is transmitted is either enabled or disabled." The Office Action concludes, on page 3, that "if the configuration is altered such that the subscriber is not to access the data, the port would be disabled." Applicants respectfully submit that this conclusion ignores the other methods for "transmitting data" (i.e., deobfuscating the data at port 314). If it is clear from paragraph [0023] that the port is either enabled or disabled, then it should likewise be clear that data is either deobfuscated at port 314 or not. Accordingly, it should be concluded that if the configuration is altered such that the subscriber is not to access the data, the port would be disabled ***or*** the obfuscated data would not be deobfuscated at the port.

In other words, paragraph [0023] describes at least two methods for transmitting data. The Office Action, on page 3, concludes that *not* transmitting data means *not* performing the first method for transmitting data. Because the described methods for transmitting data are joined with "and/or", Applicants respectfully submit that no distinction should be made among the methods for transmitting data and, therefore, if *not* transmitting data means *not* performing the first method (i.e., enabling the port), then *not* transmitting data also means *not* performing the second method (i.e., deobfuscating the data).

A person skilled in the art would have understood that if data is transmitted by "deobfuscating the data at port 314", then data is *not* transmitted by *not* "deobfuscating the data at port 314", just as a person skilled in the art would have understood that if data is transmitted by enabling the port, then data is not transmitted by not enabling the port (*see* paragraph [0023]). To "protect the data" when a subscriber violates terms of an agreement, the business entity may "'turn off' the data, such that the owner [i.e., the subscriber] is no longer able to use the data" (*see* paragraph [0023], emphasis added). The business entity may "turn off" the data "by sending a command through segment 308 that alters configuration 310", by entering "a command locally at processor 304 that alters configuration 310", or "configuration 310 may be altered automatically at the expiration of a predetermined time period" (*see* paragraph [0023]). Thus, when the data is turned "off", the configuration (310) of processor (304) may be altered, and the processor (304) may determine from the altered configuration (310) to *not* transmit the data by *not* "deobfuscating the data at port 314" (*see* paragraphs [0018]-[0024]). Accordingly, Applicants submit that Claims 1, 2, 6, 8, 10-15, 18-25, 27-31 satisfy Section 112. For at least the reasons set forth above, Applicants respectfully request that the Section 112, first paragraph, rejection of Claims 1, 2, 6, 8, 10-15, 18-25, 27-31 be withdrawn.

The rejection of Claims 18-21 under 35 U.S.C. § 112, second paragraph is respectfully traversed. Claim 18 has been amended to address the issues raised in the Office Action. Support for the amendments can be found in at least paragraphs [0023] and [0030]. Claims 19-21 depend from Claim 18. Accordingly, Applicants submit that Claims 18-21 satisfy Section 112. For at least the reasons set forth above, Applicants respectfully request that the Section 112, second paragraph, rejection of Claims 18-21 be withdrawn.

The rejection of Claims 1, 2, 6, 8, and 12-15 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0076050 to Chen et al. ("Chen") is respectfully traversed.

Chen describes a system for providing conditional access to a video on demand service used with a cable television system. The system includes a content preparation system (102) for pre-encrypting content, a video on demand system (108) that stores encrypted programs for distribution to subscribers on an on-demand basis, a conditional access system (110) for controlling one or more keys granting access to pre-encrypted content, a distribution network (112) for distributing content, and an interactive network (114) for providing two-way interaction between a set-top population (120) and video on demand system (108). The pre-encrypted content is decrypted by the set-top boxes in set-top population (120). Notably, Chen does not describe nor suggest a computer coupled to a gas turbine system.

Claim 1 recites a method of selectively controlling communication between a data source and a subscriber comprising "receiving, from the data source, a stream of obfuscated data at a supervisory processor, wherein the data source is a computer coupled to a gas turbine system . . . controlling transmission of the stream of data from the supervisory processor to the subscriber based on a configuration of the supervisory processor, wherein controlling transmission of the stream of data comprises selectively deobfuscating the obfuscated data in the stream."

Chen does not describe nor suggest a method of selectively controlling communication between a data source and a subscriber, as is recited in Claim 1. More specifically, Chen does not describe nor suggest receiving, from a data source, a stream of obfuscated data, wherein the data source comprises a computer coupled to a gas turbine system. Rather, Chen describes a conditional access system for a video on demand system used with a cable television system. Accordingly, for at least the reasons set forth above, Claim 1 is submitted to be patentable over Chen.

Claims 2, 6, and 8 depend from independent Claim 1. When the recitations of Claims 2, 6, and 8 are considered in combination with the recitations of Claim 1, Applicants submit that dependent Claims 2, 6, and 8 likewise are patentable over Chen.

Claim 12 recites a data network comprising "a first proprietary network segment configured to receive proprietary data communication that is obfuscated from a proprietary data source, wherein the proprietary data source comprises a computer coupled to a gas turbine system . . . a supervisory processor communicatively coupled to said first proprietary network segment, said processor configured to execute software instructions based on a processor configuration, said processor configured to selectively transmit subscriber data by selectively deobfuscating the subscriber data."

Chen does not describe nor suggest a data network, as is recited in Claim 12. More specifically, Chen does not describe nor suggest a first proprietary network segment configured to receive proprietary data communication that is obfuscated from a proprietary data source, wherein the proprietary data source comprises a computer coupled to a gas turbine system. Rather, Chen describes a conditional access system for a video on demand system used with a cable television system. Accordingly, for at least the reasons set forth above, Claim 12 is submitted to be patentable over Chen.

Claims 13-15 depend from independent Claim 12. When the recitations of Claims 13-15 are considered in combination with the recitations of Claim 12, Applicants submit that dependent Claims 13-15 likewise are patentable over Chen.

For the reasons set forth above, Applicants respectfully request that the Section 102 rejection of Claims 1, 2, 6, 8, and 12-15 be withdrawn.

In view of the foregoing amendments and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action are respectfully solicited.

Respectfully submitted,

Robert B. Reeser, III
Registration No. 45,548
ARMSTRONG TEASDALE LLP
7700 Forsyth Boulevard, Suite 1800
St. Louis, Missouri 63105
(314) 621-5070